

COMPLIANCE INSIGHT: THE GRAMM-LEACH-BLILEY ACT

Originally known as the Financial Modernization Act of 1999, the Gramm-Leach-Bliley Act (GLB) includes provisions to protect consumers' personal financial information held by financial institutions. The law limits the instances in which financial institutions may disclose nonpublic personal information about a consumer and requires them to disclose certain privacy policies and practices to all of its customers.

PROTECTING NON-PUBLIC PERSONAL INFORMATION

Nonpublic personal information is defined as personally identifiable information:

1. Provided by a consumer to a financial institution
2. Resulting from a transaction or service for the consumer
3. Otherwise obtained by the financial institution

Any institution that provides financial products or services to consumers must comply with the privacy provisions. This includes banks, securities firms, and insurance companies as well as companies that conduct consumer lending, money transfers, tax return preparation, credit counseling and residential real estate settlement services among other things. This is a consumer-oriented law in that financial products or services must be provided to individuals, not businesses, and be used primarily for their personal, family, or household purposes.

GLB enforcement is a function of the type of business with the Securities and Exchange Commission (SEC) acting as the enforcement body for broker/dealers, investment companies, and investment advisors. The Federal Deposit Insurance Corporation (FDIC) is the enforcing body for banks with the Federal Trade Commission (FTC) responsible for any other institution not covered by a regulator.

GLB & MESSAGING

E-mail is core to every major business process regardless of industry or company size. Everyday millions of e-mails are sent and received to and from companies that deal with consumers' personal financial information. Unchecked, this free exchange of information could breach GLB and expose the organization to legal and regulatory liability. Having no system in place to provide the required safeguards with monitoring and control of messaging represents a gaping hole in GLB compliance efforts.

Every financial institution has an obligation to respect and protect the privacy of their customers and the security and confidentiality of their nonpublic personal information. A compliance program that includes proper administrative, technical, and physical safeguards must have a system in place that can identify suspicious e-mails based on the presence of nonpublic personal information like Social Security Numbers (SSNs) or account numbers.

Every GLB compliance program must address messaging as a source of risk and potential non-compliance. Oversight and proper safeguards can be successfully achieved by deploying a policy-based system that controls the flow of personal financial information by identifying suspicious e-mails and providing visibility through reports and real-time interfaces.

About MessageGate

MessageGate is the leader in enterprise-class compliance and messaging security solutions for large organizations. The MessageGate technology has been deployed by some of the largest companies in the world helping them to monitor and control their messaging with respect to corporate policies and regulatory compliance. MessageGate empowers large, complex organizations to proactively monitor, understand, and control the risks and exposures created by the pervasive use of e-mail and other types of messaging.